AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

16. (currently amended) A method for distributed remote network monitor (dRMON) in LAN comprising:

deploying dRMON agents within ESs to be monitored said agents implementing RMON functional groups but only capturing and analyzing packets that their native ES sends or receives;

on a regular, periodic basis having the dRMON agents forward statistics and/or captured packets to a dRMON proxy or collector, existing somewhere on the WAN/LAN; and

combining received agent data thereby creating at the proxy the view that a stand-alone RMON probe would have if all the ES were on the same LAN segment with it.

17. (previously presented) The method according to claim 16 wherein said proxy can mimic the SNMP responses of a prior art non-distributed RMON probe so that existing network application management software can interact with the proxy as though the proxy were a probe.

18. (previously presented) The method according to claim 16 wherein in a default mode, ESs in the same multicast domain are treated by a proxy as though they are on one LAN segment to RMON applications to interact with the proxy though it were a probe and in an enhanced

dRMON Managers a user is provided with the ability to combine ports and hosts in order to create Virtual LAN (VLAN) definitions to cause the monitoring function to behave as though all selected hosts were on the same LAN segment being served by the same RMON probe with the dRMON collector in this embodiment creating and maintaining several such views with each appearing as one interface to conventional RMON Management applications.

19. (previously presented) The method according to claim 16 whereby said agents perform continual response time monitoring and forward the results to the Proxy.

20. (previously presented) The method according to claim 16 whereby said software utilizes native OS APIs to gather information about the ES that could not be via packet capture and analysis, such as: (1) Network protocol stack configurations and NIC configurations including problematic situations; (2) Application information ranging from what protocols an application is bound to, to its manufacturer, version, file date and time, DLLs used and their versions~~, etc.~~; (3) System information such as memory, CPU, disk space, current resource utilizations~~, etc.~~; and (4) System performance metrics.